

POWERED BY **Dialog**

Radio-relay apparatus for cable television system, has modem which registers media access control address from radio terminal side, when modem is not connected to transmission line
Patent Assignee: MASPRO DENKO KK
Inventors: SATAKE M; SHINODA M

Patent Family (1 patent, 1 country)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
JP 2003110570	A	20030411	JP 2001301507	A	20010928	200352	B

Priority Application Number (Number Kind Date): JP 2001301507 A 20010928

Patent Details

Patent Number	Kind	Language	Pages	Drawings	Filing Notes
JP 2003110570	A	JA	11	8	

Alerting Abstract: JP A

NOVELTY - A radio cable modem (20) connected to transmission line (6) of CATV system, relays data communication between radio terminals (12-16) and center apparatus (2). The modem registers media access control (MAC) address from radio terminal side, when modem is not connected to the transmission line. When modem is connected to transmission line, the access from radio terminal with non-registered MAC address is refused.

DESCRIPTION - An INDEPENDENT CLAIM is also included for bidirectional CATV system.

USE - Radio-relay apparatus connected with local area network for bidirectional cable television (CATV) system.

ADVANTAGE - Reliably prevents the unauthorized access to the apparatus by registering the unauthorized-access prevention parameters.

DESCRIPTION OF DRAWINGS - The figure shows the block diagram of a bidirectional CATV system. (Drawing includes non-English language text).

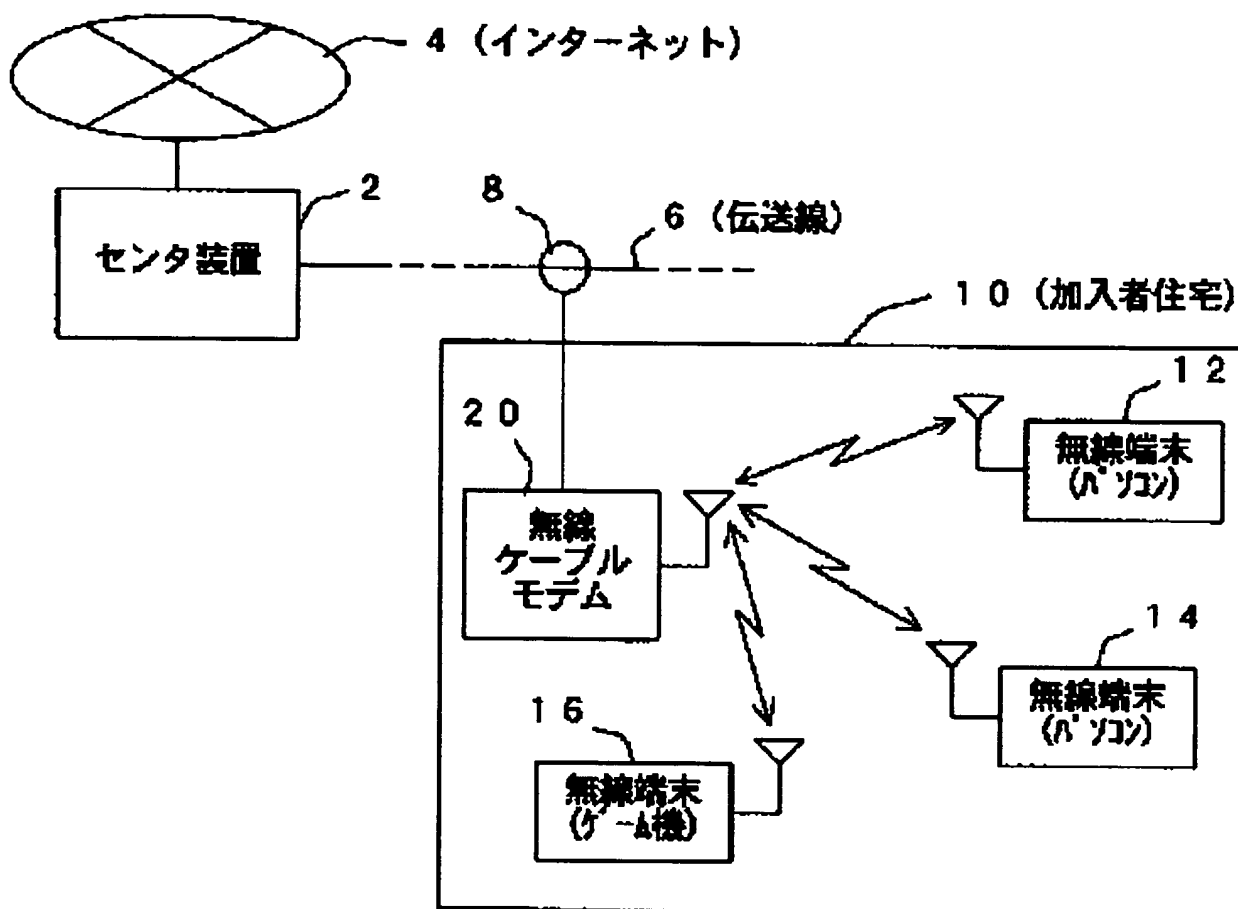
2 center apparatus

6 transmission line

12-16 radio terminals

20 cable modem

Main Drawing Sheet(s) or Clipped Structure(s)



International Classification (Main): H04L-012/28 **(Additional/Secondary):** H04B-007/15, H04B-007/26, H04L-012/46, H04Q-007/38

Original Publication Data by Authority

Japan

Publication Number: JP 2003110570 A (Update 200352 B)

Publication Date: 20030411

****WIRELESS REPEATER AND TWO-WAY CATV SYSTEM****

Assignee: MASPRO DENKOH CORP (MSPU)

Inventor: SATAKE MASA YUKI SHINODA MITSUO

Language: JA (11 pages, 8 drawings)

Application: JP 2001301507 A 20010928 (Local application)

Original IPC: H04L-12/28(A) H04B-7/15(B) H04B-7/26(B) H04L-12/46(B) H04Q-7/38(B)

Current IPC: H04L-12/28(A) H04B-7/15(B) H04B-7/26(B) H04L-12/46(B) H04Q-7/38(B)

Derwent World Patents Index

© 2006 Derwent Information Ltd. All rights reserved.

Dialog® File Number 351 Accession Number 13455108

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-110570

(P2003-110570A)

(43) 公開日 平成15年4月11日 (2003. 4. 11)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 L 12/28	3 0 0	H 0 4 L 12/28	3 0 0 A 5 K 0 3 3
H 0 4 B 7/15		12/46	Z 5 K 0 6 7
7/26		H 0 4 B 7/26	A 5 K 0 7 2
H 0 4 L 12/46		7/15	Z
H 0 4 Q 7/38		7/26	1 0 9 R
審査請求 未請求 請求項の数 8 O L (全 11 頁)			

(21) 出願番号 特願2001-301507(P2001-301507)

(22) 出願日 平成13年9月28日 (2001. 9. 28)

(71) 出願人 000113665

マスプロ電気株式会社

愛知県日進市浅田町上納80番地

(72) 発明者 佐竹 正行

愛知県日進市浅田町上納80番地 マスプロ

電気株式会社内

(72) 発明者 篠田 光生

愛知県日進市浅田町上納80番地 マスプロ

電気株式会社内

(74) 代理人 100082500

弁理士 足立 勉

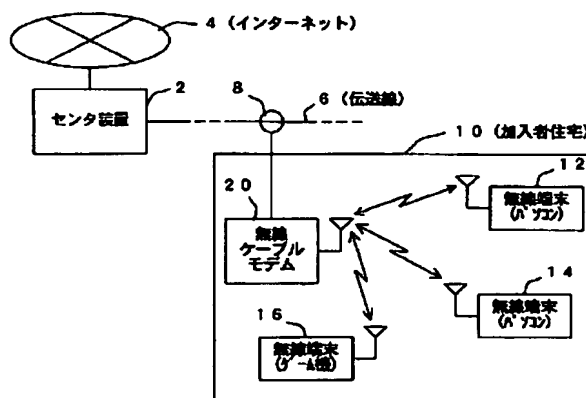
最終頁に続く

(54) 【発明の名称】 無線中継装置及び双方向CATVシステム

(57) 【要約】

【課題】 無線端末と伝送線に接続された他の通信装置との間のデータ通信を中継する無線中継装置において、無線端末を利用した第三者の不正アクセスを確実に防止し、不正アクセス防止用のパラメータを安全に登録できるようにする。

【解決手段】 双方向CATVシステムの伝送線6に接続された無線ケーブルモデム20は、加入者の無線端末12~16との間で無線通信を行うことにより、各無線端末12~16とセンタ装置2との間のデータ通信を中継する。無線ケーブルモデム20は、伝送線6に接続されていないときに、無線端末側からMACアドレスを登録できるようになっており、伝送線6に接続されると、MACアドレスが登録されていない無線端末からのアクセスを拒否する。また、無線端末のMACアドレスが何も登録されていないときには、全ての無線端末からのアクセスを拒否する。



【特許請求の範囲】

【請求項 1】 データ伝送可能な伝送線に接続され、該伝送線に接続されない無線端末との間で無線通信を行うことにより、該無線端末と前記伝送線に接続された他の通信装置との間のデータ通信を中継する無線中継装置であって、

前記データ通信の中継を行う無線端末を制限するための制限情報を記憶する記憶手段と、

該記憶手段に記憶された制限情報に基づき、前記データ通信の中継を行う無線端末を制限する無線端末制限手段と、

前記無線端末から無線にて送信されてくる登録要求に従い、前記無線端末と無線通信することにより、前記無線端末から前記制限情報を取得し、該制限情報を前記記憶手段に登録する制限情報登録手段と、

を備え、

前記無線端末制限手段は、前記記憶手段に前記制限情報が登録されていない場合に、全ての無線端末に対して、前記データ通信の中継を禁止し、

前記制限情報登録手段は、当該装置の使用者により前記制限情報の登録が許可されている場合に、前記無線端末からの登録要求を受け付け、前記制限情報の登録が許可されていない場合には、前記無線端末からの登録要求を拒否することを特徴とする無線中継装置。

【請求項 2】 前記制限情報登録手段は、当該無線中継装置が前記伝送線に接続されていないときに、前記制限情報の登録が許可されていると判断して、前記無線端末からの登録要求を受け付け、当該無線中継装置が前記伝送線に接続されているときには、前記制限情報の登録が許可されていないと判断して、前記無線端末からの登録要求を拒否することを特徴とする請求項 1 記載の無線中継装置。

【請求項 3】 前記制限情報は、少なくとも、前記データ通信の中継を許可された無線端末の MAC アドレスを含み、

前記無線端末制限手段は、前記記憶手段に前記 MAC アドレスが登録されている際には、当該無線中継装置にアクセスしてきた無線端末の MAC アドレスが前記記憶手段に登録されているか否かを判断して、登録されている場合に、該無線端末と前記通信装置との間のデータ通信の中継を許可することを特徴とする請求項 1 又は請求項 2 に記載の無線中継装置。

【請求項 4】 前記制限情報は、少なくとも、前記データ通信の中継を許可された無線端末が属するグループを表すグループ情報を含み、

前記無線端末制限手段は、前記記憶手段に前記グループ情報が登録されている際には、当該無線中継装置にアクセスしてきた無線端末が前記記憶手段に登録されたグループに属するか否かを判断して、該無線端末が該グループに属する場合に、該無線端末と前記通信装置との間の

データ通信の中継を許可することを特徴とする請求項 1 ～請求項 3 何れか記載の無線中継装置。

【請求項 5】 前記制限情報は、少なくとも、前記データ通信の中継を許可された無線端末との間の無線通信を暗号化して行うため暗号鍵を含み、

前記無線端末制限手段は、

前記記憶手段に前記暗号鍵が登録されている場合に、前記無線端末から送信されてきたデータを前記暗号鍵を用いて復号化し、前記無線端末へ送信するデータを前記暗号鍵を用いて暗号化することにより、前記通信装置との間のデータ通信が可能な無線端末を制限する暗号処理手段、

を備えたことを特徴とする請求項 1 ～請求項 4 何れか記載の無線中継装置。

【請求項 6】 前記無線端末制限手段は、前記記憶手段に前記制限情報が登録されていない場合に、当該無線中継装置にアクセスしてきた無線端末の MAC アドレスからベンダー ID を読み出し、該ベンダー ID が当該無線中継装置に付与された MAC アドレスと同じベンダー ID であれば、該無線端末と前記通信装置との間のデータ通信の中継を許可し、該ベンダー ID が異なっていれば、該無線端末と前記通信装置との間のデータ通信の中継を禁止することを特徴とする請求項 1 ～請求項 5 何れか記載の無線中継装置。

【請求項 7】 前記無線中継装置は、双方向 CATV システムの伝送線の加入者側末端部に接続され、加入者側無線端末との間で無線通信を行うことで、加入者側無線端末と双方向 CATV システムのセンタ装置との間のデータ通信を中継する無線ケーブルモデムであることを特徴とする請求項 1 ～請求項 6 何れか記載の無線中継装置。

【請求項 8】 テレビ放送信号伝送用の伝送線を介してセンタ装置と加入者側末端との間でデータ通信が可能な双方向 CATV システムにおいて、

前記伝送線の加入者側末端部に、加入者側無線端末との間で無線通信を行う無線ケーブルモデムとして、請求項 7 記載の無線中継装置を備えたことを特徴とする双方向 CATV システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、データ伝送可能な伝送線に接続され、この伝送線に接続されない無線端末との間で無線通信を行うことにより、無線端末と伝送線に接続された他の通信装置との間のデータ通信を中継する無線中継装置に関する。

【0002】

【従来の技術】 従来より、この種の無線中継装置として、例えば、有線 LAN (local area network) の伝送線に接続されて、無線端末との間で無線通信を行う無線基地局、或いは、インターネット接続サービスを行う双

方向CATVシステムの伝送線に接続されて、CATVシステムの加入者側無線端末との間で無線通信を行う無線ケーブルモデム、等が知られている。

【0003】ところで、この種の無線中継装置では、通常、無線端末との間で、米国電気電子学会の無線LANの仕様（例えば、「IEEE 802.11b」）に準拠したプロトコルで無線通信を行うように構成されていることから、LAN若しくはCATVシステムに加入していないものが、上記規格に準拠した汎用の無線端末を使って、無線中継装置にアクセスできる。

【0004】このため、上記無線中継装置には、アクセスが許可された無線端末のMACアドレス（Media Access Control address）やSSID（Service Set Identification）を登録することにより、アクセス可能な無線端末を制限したり、或いは、予め無線端末と共通の暗号鍵を登録しておき、無線端末との間でその共通の暗号鍵を利用して暗号化データを送受信することにより、無線中継装置への不正アクセスを防止することが行われている。

【0005】尚、MACアドレスは、ネットワークでホストを識別するために設定されるハードウェア固有のアドレスである。そして、このMACアドレスを利用すれば、例えば、アクセスが許可された無線端末のMACアドレスを無線中継装置に予め登録しておくことにより、その登録した無線端末以外のものから無線中継装置へのアクセスを制限する、といったことができる。

【0006】また、SSIDは、通信相手特定するための識別番号であり、このSSIDが同じ装置同士でのみ、無線通信を可能とするものである。従って、SSIDを利用すれば、例えば、アクセスが許可された無線端末と同じSSIDを無線中継装置に予め登録しておくことによって、その登録したSSIDが付与されていない無線端末から無線中継装置へのアクセスを制限する、といったことができる。

【0007】また、無線中継装置と無線端末との間で暗号化データを送受信する際には、一般に、ワイヤレスネットワークのセキュリティを確保するためのプロトコルであるWEP（Wired Equivalent Privacy）が利用される。そして、このWEPを利用すれば、無線中継装置と無線端末との間で暗号化データが送受信されることから、無線中継装置と同じ暗号鍵を有する無線端末のみが無線中継装置にアクセスすることができるようになり、無線中継装置に不正にアクセスしてきた無線端末は無線中継装置に認識されず、他の通信装置とデータ通信ができなくなる。

【0008】

【発明が解決しようとする課題】このように従来の無線中継装置は、MACアドレス、SSID、WEP等を利用して、アクセス可能な無線端末を制限できるように構成されているのであるが、従来の無線中継装置は、通

常、これらアクセス制限用のパラメータ（MACアドレス、SSID、WEP用の暗号鍵）を使用者が設定しなければ、無線中継装置と同じ仕様（例えば「IEEE 802.11b」）のプロトコルで無線通信を行う無線端末から自由にアクセスできるようになっていた。

【0009】このため、無線中継装置が接続される有線LANや双方向CATVシステムでは、上記のようなアクセス制限用のパラメータを設定していない無線中継装置を介して、第三者による不正侵入が行われることがあった。一方、こうした問題を防止するためには、無線中継装置を、上述した不正アクセスを防止するためのパラメータが設定されていない場合に、全ての無線端末のアクセスを禁止するように構成すればよい。

【0010】しかしながら、このように上記パラメータが設定されていない場合に、無線端末から無線中継装置へのアクセスを全て禁止すると、無線端末を利用して上記パラメータを設定することができなくなり、使い勝手が悪いという問題が生じる。また、この場合、上記パラメータの設定を、伝送線を介して無線中継装置に接続される通信装置から行うようにすることもできるが、このようにすると、伝送線に接続可能な第三者から上記パラメータが不正に設定される虞がある。

【0011】これに対して、上記パラメータの設定だけは、無線通信によって無線端末側から行えるようにすることもできるが、無線中継装置をこのように構成すると、今度は、第三者が自分の無線端末を利用できるように上記パラメータを設定することが可能となり、第三者による無線端末を使った不正アクセスを防止することができなくなってしまう。

【0012】本発明は、こうした問題に鑑みなされたものであり、有線LANや双方向CATVシステム等の伝送線に接続されて、無線端末と伝送線に接続された他の通信装置との間のデータ通信を中継する無線中継装置において、無線端末を利用した第三者の不正アクセスを確実に防止でき、しかもその不正アクセス防止用のパラメータを、無線端末を利用して安全に登録できるようにすることを目的とする。

【0013】

【課題を解決するための手段及び発明の効果】かかる目的を達成するためになされた請求項1に記載の無線中継装置は、データ通信の中継を行う無線端末を制限するための制限情報を記憶する記憶手段を備え、無線端末制限手段が、その記憶手段に記憶された制限情報に基づき、データ通信の中継を行う無線端末を制限し、しかも、記憶手段に制限情報が登録されていない場合には、全ての無線端末に対して、データ通信の中継を禁止する。

【0014】このため、本発明の無線中継装置を用いれば、記憶手段に記憶された制限情報により制限を受けない無線端末のみが、伝送線に接続された他の通信装置との間のデータ通信が可能となり、第三者が自分の所有す

る無線端末を利用して無線中継装置を不正使用することは不可能になる。

【0015】一方、記憶手段への制限情報の登録は、無線端末側から登録要求を無線にて送信することにより起動される制限情報登録手段を介して、無線端末側から行うことができる。そして、本発明において、この制限情報登録手段は、使用者により制限情報の登録が許可されている場合にだけ、無線端末からの登録要求を受け付け、制限情報の登録が許可されていない場合には無線端末からの登録要求を拒否するように構成されることから、第三者が自分の無線端末を利用して記憶手段に制限情報を書き込むことはできなくなる。

【0016】よって、本発明の無線中継装置によれば、無線端末を利用した第三者の不正アクセスを確実に制限でき、しかもその不正アクセス制限用の制限情報を無線端末を利用して安全に登録できることになる。ここで、制限情報登録手段は、使用者により制限情報の登録が許可されている場合にだけ無線端末からの登録要求を受け付けるが、このためには、無線中継装置に、使用者が制限情報の登録を許可するか否かを手動操作で切り替えるための切換スイッチを設けるようにしてもよい。

【0017】しかし、このような切換スイッチを設けると、制限情報登録後の使用者の操作忘れによって、第三者が自分の無線端末を利用して記憶手段に制限情報を登録できるようになることも考えられるので、より好ましくは、制限情報登録手段を、請求項2に記載のようにする

とよい。

【0018】即ち、請求項2に記載の無線中継装置では、制限情報登録手段は、当該無線中継装置が伝送線に接続されていないときに、制限情報の登録が許可されると判断して、無線端末からの登録要求を受け付け、当該無線中継装置が伝送線に接続されているときには、制限情報の登録が許可されていないと判断して、無線端末からの登録要求を拒否するように構成される。

【0019】この結果、請求項2に記載の無線中継装置によれば、無線端末を利用した制限情報の登録は、当該無線中継装置を伝送線に接続する前、若しくは、当該無線中継装置を伝送線から外してから行う必要があり、当該無線中継装置が伝送線に接続されているときには、制限情報の登録を行うことができなくなるので、当該無線中継装置が伝送線に接続されて通常動作状態にあるときには、第三者が自分の無線端末を利用して記憶手段に制限情報を書き込むことはできなくなり、第三者による無線中継装置の不正使用をより確実に防止できる。

【0020】一方、記憶手段に登録する制限情報としては、請求項3に記載のように、データ通信の中継を許可された無線端末のMACアドレスであっても、請求項4に記載のように、データ通信の中継を許可された無線端末が属するグループを表すグループ情報（例えば、上述のSSID等）であっても、請求項5に記載のように、

データ通信の中継を許可された無線端末との間の無線通信を暗号化して行うため暗号鍵（例えば、上述のWEPでデータ通信に制限をかけるための暗号鍵）であっても、或いは、これらのパラメータを組み合わせてもよい。

【0021】そして、MACアドレスを制限情報として記憶手段に登録できるように構成した際には、無線端末制限手段を、記憶手段にMACアドレスが登録されている際に、当該無線中継装置にアクセスしてきた無線端末のMACアドレスが記憶手段に登録されているか否かを判断して、登録されている場合に、その無線端末と伝送線に接続された通信装置との間のデータ通信の中継を許可するように構成すればよい（請求項3参照）。

【0022】また、SSID等のグループ情報を制限情報として記憶手段に登録できるように構成した際には、無線端末制限手段を、記憶手段にグループ情報が登録されている際に、当該無線中継装置にアクセスしてきた無線端末が記憶手段に登録されたグループに属するか否かを判断して、無線端末が記憶手段に登録されたグループに属する場合に、その無線端末と伝送線に接続された通信装置との間のデータ通信の中継を許可するように構成すればよい（請求項4参照）。

【0023】一方、WEP等のプロトコルで利用される暗号鍵を制限情報として記憶手段に登録できるように構成した際には、請求項5に記載のように、無線端末制限手段に暗号処理手段を設けるようにすればよい。つまり、請求項5に記載の無線中継装置において、暗号処理手段は、記憶手段に暗号鍵が登録されている際に、無線端末から送信されてきたデータを、記憶手段に登録された暗号鍵を用いて復号化し、無線端末へ送信するデータを、記憶手段に登録された暗号鍵を用いて暗号化することから、通信装置との間のデータ通信が可能な無線端末は、記憶手段に登録されたものと同じ暗号鍵を用いて送信データの暗号化、受信データの復号化を行う無線端末に制限され、この暗号鍵を用いてデータ通信を行うことのできない無線端末は、無線中継装置を利用したデータ通信を行うことができなくなる。

【0024】ところで、請求項1～請求項5に記載の無線中継装置において、記憶手段に制限情報（MACアドレス、SSID等のグループ情報、WEP等のプロトコルで利用される暗号鍵等）が登録されていなければ、無線端末制限手段は、無線中継装置にアクセスしてきた全ての無線端末に対して、伝送線に接続された他の通信装置との間のデータ通信の中継を禁止するが、このような無線中継装置は、無線端末を操作して無線中継装置に制限情報を登録することができない使用者にとっては極めて使い勝手の悪いものとなってしまふ。

【0025】そこで、本発明（請求項1～請求項5）の無線中継装置においては、無線端末制限手段を、請求項6に記載のように構成してもよい。即ち、請求項6に記

載の無線中継装置において、無線端末制限手段は、記憶手段に制限情報が登録されていない場合に、当該無線中継装置にアクセスしてきた無線端末の MAC アドレスからベンダー ID を読み出し、そのベンダー ID が当該無線中継装置に付与された MAC アドレスと同じベンダー ID である場合に限り、その無線端末と通信装置との間のデータ通信の中継を許可するように構成してもよい。

【0026】つまり、MAC アドレスは、48 ビット（換言すれば 6 バイト）のデジタルデータからなり、そのうちの前半 24 ビットが IEEE（米国電気電子学会）で管理された管理組織固有の ID（ベンダー ID）、後半 24 ビットが無線端末（若しくはパーソナルコンピュータ等の情報機器を無線端末として利用するために装着される NIC（ネットワークインターフェイスカード））固有の番号、となっていることから、請求項 6 に記載の無線中継装置では、この MAC アドレスを構成しているベンダー ID を利用して、無線中継装置を利用可能な無線端末を制限するのである。

【0027】そして、このようにすれば、無線中継装置の所有者は、無線中継装置を購入する際、無線中継装置とベンダー ID が同じ無線端末（若しくは NIC）を購入すれば、これらをそのまま使って、伝送線上の他の通信装置との間でデータ通信を行うことができることから、無線中継装置の使い勝手を向上できる。

【0028】尚、この場合、無線中継装置に付与された MAC アドレスと同じベンダー ID の MAC アドレスを有する無線端末（換言すれば、無線中継装置と製造会社が同じ無線端末）については、何ら制限を受けることなく、無線中継装置を利用できることになるが、無線中継装置を不正に利用しようとする第三者は、この無線中継装置と同じ製造会社から供給される無線端末を準備しなければならないため、従来に比べて、無線中継装置の不正使用を防止できる。

【0029】次に、請求項 7 に記載の無線中継装置は、上述した本発明（請求項 1～請求項 6）の無線中継装置を、双方向 CATV システムの伝送線の加入者側末端部に接続されて、加入者側無線端末と双方向 CATV システムのセンタ装置との間のデータ通信を中継する無線ケーブルモデムに適用したものである。

【0030】そして、このように本発明（請求項 1～請求項 6）に無線中継装置を双方向 CATV システム用の無線ケーブルモデムに適用した場合、この無線ケーブルモデムを使って、双方向 CATV システムにて提供されるインターネットサービス等のデータ通信サービスを加入者以外の者が不正に利用できるようになるのを防止し、延いては、この不正利用に伴い正規の加入者が不利益を被るのを防止できる。

【0031】また次に、請求項 8 に記載の発明は、請求項 7 に記載の無線中継装置（無線ケーブルモデム）を伝

送線の加入者側末端部に備え、無線中継装置（無線ケーブルモデム）を利用して加入者側無線端末とセンタ装置との間のデータ通信を行えるようにした双方向 CATV システムに関するものである。

【0032】そして、この双方向 CATV システムによれば、双方向 CATV システムが提供するインターネットサービス等のデータ通信サービスを、加入者以外の者が不正に利用するのを防止し、この不正利用に伴い正規の加入者が不利益を被るのを防止できる。

【0033】

【発明の実施の形態】以下に、本発明の実施例を図面と共に説明する。図 1 は、本発明が適用された実施例の双方向 CATV システムの概略構成図であり、図 2 は、この双方向 CATV システムの伝送線 6 の加入者側末端部に接続された無線ケーブルモデム（本発明の無線中継装置に相当する）の構成を表すブロック図である。

【0034】図 1 に示すように、本実施例の双方向 CATV システムは、インターネット 4 に接続され、加入者側の端末装置（図では、無線端末 12、14、16）からの要求に従い、その端末装置をインターネット 4 に接続する ISP（インターネットサービスプロバイダ）としての機能を有するセンタ装置 2 を備える。

【0035】そして、このセンタ装置 2 から出力される所定周波数帯（例えば、70 MHz～770 MHz）の下り信号（テレビ放送信号やデータ通信の信号）は伝送線 6 を介して加入者側の端末装置へと下り方向に伝送され、加入者側の端末装置から出力された所定周波数帯（例えば、5 MHz～42 MHz）の上り信号（データ通信の信号）は、下り信号と同じ伝送線 6 を介して、センタ装置 2 側へと上り方向に伝送される。

【0036】また、伝送線 6 には、下り信号及び上り信号を夫々増幅し、必要に応じて伝送線 6 を分岐する図示しない増幅器や分岐増幅器が複数設けられ、更に、加入者住宅 10 の近傍で伝送線 6 を加入者住宅 10 まで引き込むためのタップオフ（分岐器）8 も多数設けられている（図ではそのうちの一つを記載）。

【0037】このため、本実施例の双方向 CATV システムにおいて、インターネット接続サービスに加入している加入者は、タップオフ 8 や図示しない保安器等を介して加入者住宅 10 内に引き込まれた伝送線 6 の末端部に、有線のケーブルモデム若しくは図 1 に示す無線ケーブルモデム 20 を接続し、更に、このケーブルモデムに、インターネットにアクセス可能な情報端末（パーソナルコンピュータ、ゲーム機等）を有線若しくは無線で接続することにより、この情報端末を使ってインターネットを利用できる。

【0038】また、伝送線 6 の末端部に無線ケーブルモデム 20 が接続された加入者住宅 10 では、情報端末として、無線 LAN の通信機能を有する無線端末、若しくは、無線 LAN 用の NIC（PC カードやパーソナルコ

ンピュータの拡張ボード)をパーソナルコンピュータ(パソコン)やゲーム機に組み込むことによって構成される無線端末、を利用することにより、無線ケーブルモデム20を介して、複数の無線端末12、14、16…をインターネットに接続できる。

【0039】つまり、無線ケーブルモデム20は、無線LANの一般的な仕様である「IEEE802.11b」に準拠したプロトコルで複数の無線端末12、14、16…と無線通信を行うことで、これら各無線端末12、14、16…とセンタ装置2内のISP用の通信装置との間のデータ通信を中継する無線中継装置であり、各無線端末12、14、16…は、この無線ケーブルモデム20を介して、双方向CATVシステムが提供するISPとしてのサービス(つまりインターネット接続サービス)を享受できるのである。

【0040】次に、このような中継機能を有する無線ケーブルモデム20は、図2に例示するように、CATV側送受信部30と、デジタル変・復調部40と、暗号処理部50と、無線送受信部60と、制御部70と、EEPROM等からなる不揮発性のメモリ80と、を備える。

【0041】ここで、CATV側送受信部30は、同軸コネクタCNを介して、同軸ケーブルからなる伝送線6の末端部に接続され、伝送線6を介して、センタ装置2内の通信装置との間で双方向通信を行うためのものであり、センタ装置2側から送信されてきた下り信号の中からデータ通信用の下り信号を抽出する選局部34と、デジタル変・復調部40から出力されたセンタ装置2への送信信号を所定周波数帯の上り信号に周波数変換する周波数変換部36と、これら各部34、36と同軸コネクタCNとの間に設けられて、センタ装置2側から送信されてきた下り信号を選局部34に入力し、周波数変換部36から出力された上り信号を同軸コネクタCN側に出し、これら各信号の周り込みを防止する信号分離部32と、から構成されている。

【0042】また、デジタル変・復調部40は、CATV側送受信部30(詳しくは選局部34)から入力される下り信号からデジタルデータ(下りデータ)を復調し、暗号処理部50に出力するデジタル復調部42と、暗号処理部50から入力されるセンタ装置2側への送信データ(上りデータ)を送信用の信号に変調し、CATV側送受信部30(詳しくは周波数変換部36)に出力するデジタル変調部44と、から構成されている。

【0043】次に、暗号処理部50は、制御部70が実行する後述の端末登録処理によって上述したWEP用の暗号鍵が設定されているときに、外部の無線端末12、14、16…との間で暗号化データを送受信できるようにするためのものであり、デジタル変・復調部40(詳しくはデジタル復調部42)から入力された下りデータを暗号鍵を用いて暗号化して無線送受信部60に出力す

る暗号化部52と、無線送受信部60から入力される無線端末12、14、16…からの受信データ(上りデータ)を暗号鍵を用いて復号化し、デジタル変・復調部40(詳しくはデジタル変調部44)に出力する復号化部54と、から構成されている。

【0044】また、無線送受信部60は、アンテナATを介して「IEEE802.11b」に準拠した2.4GHz帯の無線電波を送受信することにより、無線端末12、14、16…との間で無線通信を行うためのものであり、制御部70は、無線端末12、14、16…とセンタ装置2内の通信装置との間で行われるデータ通信を中継できるように上記各部30、40、50、60を制御するためのものである。

【0045】そして、制御部70は、CPU、RAM、ROM等からなるマイクロコンピュータにて構成されており、上記中継のために行う上記各部30、40、50、60の制御に加えて、当該無線ケーブルモデム20にてデータ通信の中継を行う無線端末を予め登録された無線端末12、14、16、…に制限するための端末登録・監視処理を実行する。

【0046】図3に示すように、この端末登録・監視処理では、まず、S110(Sはステップを表す)にて、CATV側送受信部30の選局部34から出力される下り信号を監視し、続くS120にて、選局部34から下り信号が出力されているか否かを判断することにより、無線ケーブルモデム20が同軸コネクタCNを介して伝送線6に接続されているか否かを判断する。

【0047】そして、無線ケーブルモデム20が伝送線6に接続されていない場合は、S130に移行して、当該無線ケーブルモデム20を利用可能な無線端末を、無線端末側からの登録要求に応じて登録する端末登録処理を実行し、逆に、無線ケーブルモデム20が伝送線6に接続されている場合は、続くS140に移行して、S130の端末登録処理の実行により、当該無線ケーブルモデム20を利用可能な無線端末が既に登録されているか否か(換言すれば無線端末の登録データが有るか否か)を判断する。

【0048】尚、本実施例では、S140において、無線端末のMACアドレスが一つでも登録されているか否かによって、無線端末の登録データの有無を判断するようにされている。そして、S140にて、無線端末の登録データは存在しないと判断されると、S160にて全ての無線端末からのアクセスを禁止した後、当該処理を一旦終了し、逆に、S140にて、無線端末の登録データが有ると判断されると、続くS150に移行する。そして、S150では、当該無線ケーブルモデム20にアクセスしてきた無線端末が、先に登録された無線端末であるかどうかを監視し、登録されている無線端末に対してのみデータ通信の中継を許可する、端末監視処理を実行する。

【0049】次に、S130にて実行される端末登録処理は、図4に示す手順で実行される。図4に示すように、端末登録処理では、まずS210にて、無線送受信部60が無線端末からの送信データ（上りデータ）を受信したか否かを判断することにより、無線端末から上りデータが送信されてくるのを待つ。そして、S210にて、無線送受信部60が無線端末からの上りデータを受信したと判断すると、S220に移行して、暗号処理部50から出力される上りデータを取り込み、この上りデータから、この上りデータの送信先アドレス（IPアドレス）を取得する。

【0050】尚、既述したように、暗号処理部50は、暗号鍵が設定されている場合に、下りデータの暗号化及び上りデータの復号化を行うものであり、暗号鍵が設定されていなければ、これら各データをそのまま入出力することから、S220の処理実行時に、暗号鍵が設定されていなければ、制御部70には、無線送受信部60が受信した上りデータがそのまま取り込まれ、逆に、暗号鍵が設定されていれば、制御部70には、復号化部54にて復号化処理が施された上りデータが取り込まれる。

【0051】次に、続くS230では、上りデータから取得した送信先アドレスが、当該制御部70に予め設定されたIPアドレス（自己アドレス）であるか否か、換言すれば当該制御部70に対する無線端末の登録要求が送信されてきたか否かを判断する。そして、S230にて、上りデータから取得した送信先アドレスが自己アドレスであると判断されると、S240に移行して、今回上りデータを送信してきた無線端末に端末登録用のWebページを表示させるための端末登録用データを生成し、これを暗号化部52に出力することにより、暗号化部52、及び、無線送受信部60を介して、今回上りデータを送信してきた無線端末に端末登録用データを送信し、逆に、S230にて、上りデータから取得した送信先アドレスが自己アドレスではないと判断されると、そのまま当該処理を一旦終了する。

【0052】ここで、S240の処理は、端末登録用のWebサーバとしての機能を実現する処理であり、この処理の実行により、上りデータを送信してきた無線端末には、図5に例示する端末登録用のWebページが表示される。図5に例示するように、このWebページは、無線ケーブルモデム20の利用可能端末を特定するための識別情報であるMACアドレスを登録するためのMACアドレス登録領域72と、無線ケーブルモデム20が属する無線ネットワークの識別情報であるSSIDを登録するためのSSID登録領域74と、無線ケーブルモデム20が無線端末との間で無線通信を行う際に通信データを暗号化するWEPを利用するか否か、及びWEPを利用するのであれば、暗号鍵に64ビットのデータを使うか128ビットのデータを使うかを指定するためのWEP選択領域76と、WEPの利用を選択した際に、

暗号鍵の登録ページを要求するための登録ページ要求領域78とから構成されている。

【0053】このため、使用者は、無線端末に表示されたWebページを見ながら、MACアドレス、SSID、WEP利用の有無を設定でき、WEPを利用する際には、暗号鍵の登録ページを要求して、その登録ページで、任意の暗号鍵を設定できる。

【0054】尚、本実施例では、無線ケーブルモデム20を利用するためには、少なくとも、無線端末のMACアドレスを登録することが必須とされており、SSID及びWEPについては、任意に設定できるようにされている。次に、S240にて、端末登録用のWebページ（端末登録用データ）を送信すると、今度は、S250に移行して、暗号処理部50から出力される上りデータを監視することにより、S240で端末登録用データを送信した無線端末側から上述したMACアドレス、SSID、WEP等の登録情報（本発明の制限情報に相当する）が送信されてくるのを待ち、この登録情報を受信すると、続くS260にて、その受信した登録情報（受信情報）は正常か否かを判断する。そして、受信情報が正常であれば、S270に移行して、その受信情報をメモリ80に格納することにより、無線ケーブルモデム20を使用可能な無線端末を登録する。

【0055】尚、無線端末からの登録情報の送信は、図5に示したWebページ上で、「適用」若しくは「取消」を指定することにより行われる。そして、S270では、Webページ上で「適用」が選択されることにより送信されてきた登録情報については、新規登録する情報として受け付け、Webページ上で「取消」が選択されることにより送信されてきた登録情報については、既に登録された情報の取消指令として受け付ける。

【0056】また、S270において、無線端末から送信されてきた登録情報の内、MACアドレス及びSSIDについては、無線ケーブルモデム20を利用可能な無線端末を特定するための情報としてそのままメモリ80に記憶するが、WEP利用の有無及び利用する際の暗号鍵を表す情報については、暗号処理部50を動作させるのに必要な情報であるので、メモリ80に記憶するだけでなく、暗号処理部50の制御情報として、暗号処理部50にも設定する。

【0057】そして、このようにS270にて、受信情報に従い当該無線ケーブルモデム20を利用可能な無線端末を登録するか、或いは、S260にて、受信情報に異常があると判断すると、S280に移行して、受信情報の登録結果を無線端末側に送信し、当該処理を一旦終了する。

【0058】次に、図6は、図3に示すS150にて実行される端末監視処理を表すフローチャートである。図6に示すように、端末監視処理では、まずS310にて、無線送受信部60が無線端末からの送信データ（上

りデータ)を受信したか否かを判断することにより、無線端末から上りデータが送信されてくるのを待つ。そして、S310にて、無線送受信部60が無線端末からの上りデータを受信したと判断すると、S320に移行して、暗号処理部50から出力される上りデータを取り込み、この上りデータから端末識別情報を取得する。この端末識別情報は、基本的には、無線端末のMACアドレスであるが、上記端末登録処理によってメモリ80に当該無線ケーブルモデム20が属する無線ネットワークの識別情報であるSSIDが登録されていれば、上りデータからSSIDも取得する。

【0059】そして、続くS330では、上りデータから取得した無線端末の識別情報であるMACアドレスがメモリ80に登録されているか否かを判断すると共に、メモリ80にSSIDが登録されていれば、上りデータから取得したSSIDがその登録されたSSIDと一致するか否かを判断することにより、今回上りデータを送信してきた(換言すれば当該無線ケーブルモデム20にアクセスしてきた)無線端末は、当該無線ケーブルモデム20を利用可能な無線端末として登録されているか否かを判断する。

【0060】そして、S330にて、無線端末が登録済みであると判断されると、S340にて、その無線端末から当該無線ケーブルモデム20へのアクセスを許可して、当該処理を一旦終了し、逆に、S330にて、無線端末が登録されていないと判断されると、S350にて、その無線端末から当該無線ケーブルモデム20へのアクセスを禁止して、当該処理を一旦終了する。

【0061】尚、上記端末登録処理により当該無線ケーブルモデム20へのアクセスを制限する制限情報としてWEPが設定されている場合には、暗号処理部50が、登録された暗号鍵を使って上りデータの復号化を行うことから、上りデータを送信してきた無線端末が、同じ暗号鍵を使って上りデータを暗号化していなければ、暗号処理部50で上りデータを復元できない。従って、当該無線ケーブルモデム20へのアクセスを制限する制限情報としてWEPが設定されている場合、無線ケーブルモデム20と同じWEP設定がなされていない無線端末については、上りデータから端末識別情報を取得することができず、アクセスが禁止されることになる。

【0062】以上説明したように、本実施例の双方向CATVシステムにおいては、加入者住宅10に、加入者側の複数の無線端末12、14、16…との間で無線通信を行うことにより、無線端末12、14、16…とセンタ装置2内の通信装置との間のデータ通信を中継する無線ケーブルモデム20が設置されている。

【0063】そして、この無線ケーブルモデム20は、データ通信の中継を行う無線端末を制限するために、当該無線ケーブルモデム20を利用可能な無線端末のMACアドレスを予め登録しておき、MACアドレスが登録

されていない無線端末については、データ通信の中継を禁止し、しかも、無線端末のMACアドレスが登録されていない場合には(S140:NO)、データ通信の中継動作を実行しないようにされている。このため、本実施例の無線ケーブルモデム20を用いれば、MACアドレスが登録されていない無線端末からセンタ装置2への不正アクセスを確実に防止できる。

【0064】一方、本実施例の無線ケーブルモデム20では、上記制限情報を登録するための端末登録処理を、無線ケーブルモデム20が伝送線6から外されているときに限って実行するようにされており、無線ケーブルモデム20が伝送線6に接続される通常時には、当該無線ケーブルモデム20を利用可能な無線端末を登録できないようになっている。このため、無線ケーブルモデム20を不正使用するために、第三者が自分の無線端末のMACアドレスを登録できる機会は殆どなく、これによっても、第三者の無線端末からセンタ装置2への不正アクセスを防止できる。

【0065】また、特に、本実施例の無線ケーブルモデム20は、データ通信の中継を行う無線端末を制限するための制限情報として、MACアドレス以外にも、SSIDやWEP用の暗号鍵を任意に登録できるようにされているため、これらを登録することにより、第三者の無線端末からセンタ装置2への不正アクセスをより確実に防止できる。

【0066】そして、本実施例の無線ケーブルモデム20によれば、双方向CATVシステムの加入者が、無線ケーブルモデム20を使用した無線LANを自宅で構築しても、第三者による不正アクセスを確実に防止できることから、加入者以外の者が無線端末を使ってセンタ装置2へ不正アクセスすることによって、正規の加入者が不利益を被るのを防止できる。

【0067】よって、本実施例の無線ケーブルモデム20を利用すれば、インターネット接続サービス等を行う双方向CATVシステムの信頼性を向上し、加入者にとって安心して利用できる双方向CATVシステムを実現できることになる。尚、本実施例においては、図3に示すS110~S130の一連の処理が、本発明の制限情報登録手段として機能し、S140及びS150の一連の処理が、本発明の無線端末制限手段として機能する。また、暗号処理部50は、本発明(特に請求項5)の暗号処理手段に相当し、不揮発性のメモリ80は、本発明の記憶手段に相当する。そして、本実施例において、記憶手段を不揮発性のメモリ80にて構成しているのは、無線ケーブルモデム20への電源供給を遮断した際に、一旦登録した制限情報が消失するのを防止するためである。

【0068】以上、本発明の一実施例について説明したが、本発明は、上記実施例に限定されるものではなく、種々の態様を採ることができる。例えば、上記実施例で

10

20

30

40

50

は、データ通信の中継を行う無線端末を制限するための制限情報を登録する端末登録処理を、無線ケーブルモデム 20 が伝送線 6 から外されているときに限って実行するように構成したが、例えば、この端末登録処理は、使用者が無線ケーブルモデム 20 に設けられた登録スイッチ (SW) を手でオンした際に、実行するようにしてもよい。そして、この場合、端末登録・監視処理としては、例えば図 7 に示す手順で実行するようにすればよい。

【0069】即ち、図 7 に示す端末登録・監視処理では、まず、S410 にて、無線送受信部 60 が無線端末からの送信データ (上りデータ) を受信したか否かを判断することにより、無線端末から上りデータが送信されてくるのを待つ。そして、S410 にて、無線送受信部 60 が無線端末からの上りデータを受信したと判断すると、S420 に移行して、暗号処理部 50 から出力される上りデータを取り込み、この上りデータから、この上りデータの送信先アドレス (IP アドレス) を取得する。

【0070】また、続く S430 では、上りデータから取得した送信先アドレスが、当該制御部 70 に予め設定された IP アドレス (自己アドレス) であるか否かを判断し、上りデータから取得した送信先アドレスが自己アドレスであれば、S440 にて、登録 SW がオンされているか否かを判断する。

【0071】そして、登録 SW がオンされていれば、使用者により無線端末の登録が許可されていると判断して、S130' にて端末登録処理を実行した後、当該処理を一旦終了し、逆に、登録 SW がオンされていなければ (換言すれば、無線端末の登録が許可されていなければ)、当該処理を一旦終了する。尚、S130' の端末登録処理では、図 4 に示した S210~S230 の処理を実行する必要はないので、S240~S280 の処理が実行される。

【0072】一方、S430 にて、上りデータから取得した送信先アドレスが自己アドレスではないと判断された場合には、S140 に移行して、メモリ 80 内に無線端末の登録データ (MAC アドレス) が有るか否かを判断し、S140 にて、メモリ 80 内に無線端末の登録データは存在しないと判断されると、当該処理を一旦終了し、逆に、S140 にて、無線端末の登録データが有ると判断されると、続く S150' に移行して、端末監視処理を実行する。尚、S150' の端末監視処理では、図 6 に示した S310 の判定処理を実行する必要はないので、S320~S350 の処理が実行される。

【0073】このように、図 7 に示した端末登録・監視処理では、上りデータから取得した送信先アドレスが自己アドレスであり、無線端末からその登録要求を受けた際に、登録 SW がオンされているか否か、つまり、使用者により無線端末の登録が許可されているか否かを判断

し、無線端末の登録が許可されているときにだけ、S130' の端末登録処理を実行するようにしている。

【0074】そして、端末登録・監視処理を、このように実行するようにしても、使用者が登録 SW をオフするのを忘れなければ、第三者が自分の無線端末の MAC アドレスを無線ケーブルモデム 20 に登録できる機会は殆どなく、上記実施例と同様の効果を得ることができる。

【0075】一方、上記実施例では、S140 の判定処理にて、メモリ 80 に MAC アドレスが登録されていないと判断されると、S160 にて全ての無線端末からのアクセスを禁止するものとして説明したが、S160 の処理に代えて、図 8 に示す処理 (S160') を実行するようにしてもよい。

【0076】即ち、この処理 (S160') では、S140 の判定処理にて否定判断されると、上りデータから無線端末の MAC アドレスを取得し (S510)、その取得した MAC アドレスを構成しているベンダー ID が、当該無線ケーブルモデム 20 に付与された MAC アドレスのベンダー ID と一致するか否かを判断して (S520)、ベンダー ID が一致している場合には、その無線端末からのアクセスを許可し (S530)、ベンダー ID が一致していなければ、その無線端末からのアクセスを禁止する (S540)。

【0077】そして、このようにすれば、無線ケーブルモデム 20 の所有者は、無線ケーブルモデム 20 を購入する際、これとベンダー ID が同じ無線端末 (若しくは NIC) を購入すれば、これらをそのまま使って、センタ装置 2 内の通信装置とデータ通信を行うことができるようになり、無線ケーブルモデム 20 の使い勝手を向上できる。

【0078】尚、この場合、無線ケーブルモデム 20 に付与された MAC アドレスと同じベンダー ID の MAC アドレスを有する無線端末については、何ら制限を受けることなく、無線ケーブルモデム 20 を利用できるようになるが、無線ケーブルモデム 20 を不正に利用しようとする第三者は、この無線ケーブルモデム 20 と同じベンダー ID の無線端末を準備しなければならないため、第三者による無線ケーブルモデム 20 の不正使用を防止できる。

【0079】また次に、上記実施例では、本発明の無線中継装置を双方向 CATV システムで用いられる無線ケーブルモデム 20 に適用した場合について説明したが、本発明の無線中継装置は、無線端末から有線 LAN に接続するのに用いられる無線 LAN 用の基地局等にも適用できるのは、いうまでもない。

【図面の簡単な説明】

【図 1】 実施例の双方向 CATV システムの概略構成図である。

【図 2】 実施例の無線ケーブルモデムの構成を表すブロック図である。

17

【図3】 実施例の無線ケーブルモデムで実行される端末登録・監視処理を表すフローチャートである。

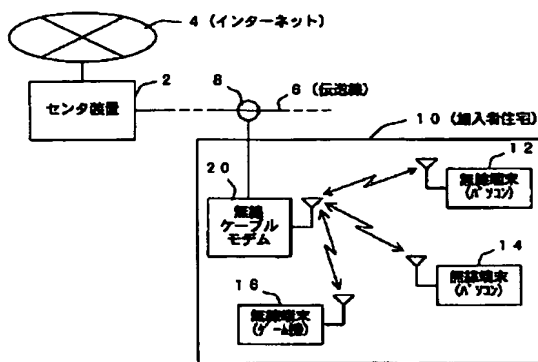
【図4】 図3のS130にて実行される端末登録処理を表すフローチャートである。

【図5】 図4の端末登録処理で加入者側の無線端末に提供されるWebページの一例を表す説明図である。

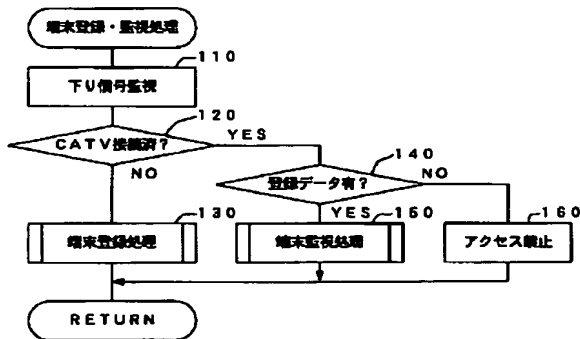
【図6】 図3のS150にて実行される端末監視処理を表すフローチャートである。

【図7】 端末登録・監視処理の他の実施例を表すフローチャートである。

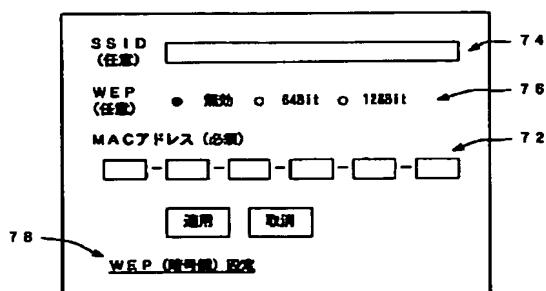
【図1】



【図3】



【図5】



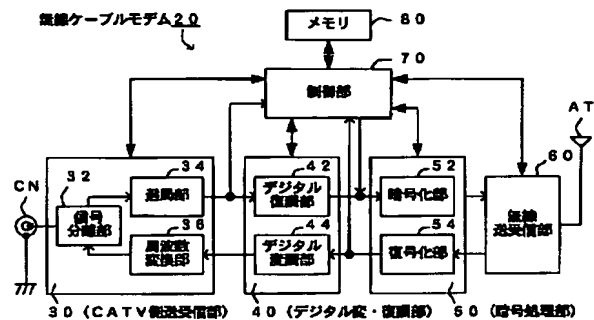
18

【図8】 図3に示した端末登録・監視処理の一部変形例を表すフローチャートである。

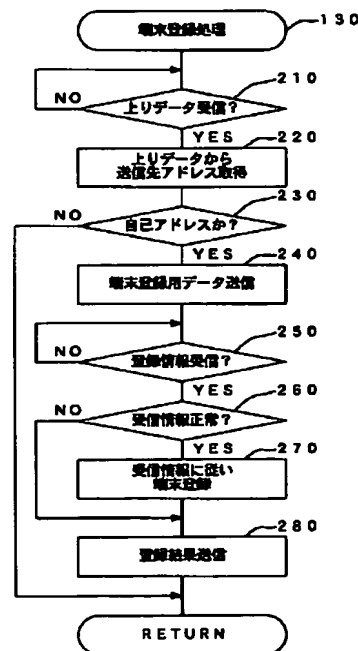
【符号の説明】

2…センタ装置、4…インターネット、6…伝送線、8…タップオフ、10…加入者住宅、12、14、16…無線端末、20…無線ケーブルモデム、30…CATV側送受信部、40…デジタル変・復調部、50…暗号処理部、60…無線送受信部、70…制御部、80…メモリ。

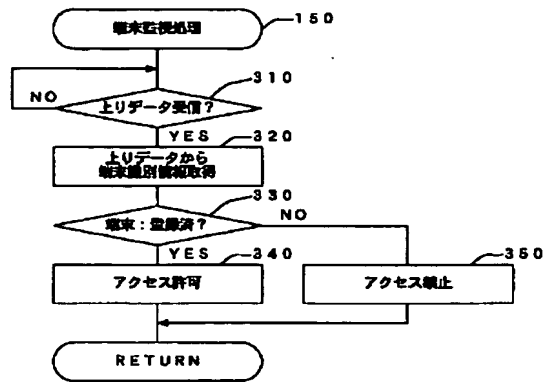
【図2】



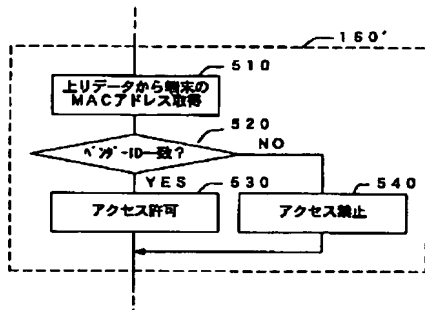
【図4】



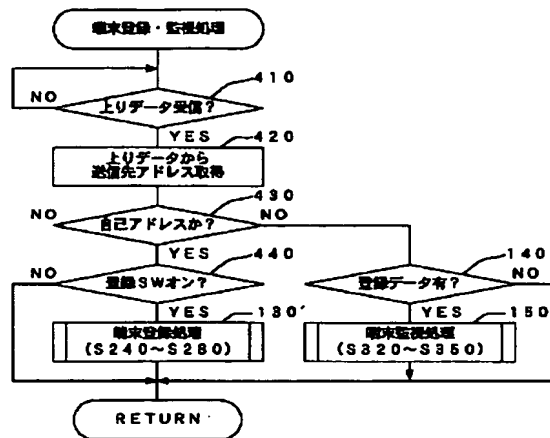
【図6】



【図8】



【図7】



フロントページの続き

Fターム(参考) 5K033 AA08 BA07 DA05 DA17 DB19
 5K067 AA35 BB21 DD13 EE02 EE06
 HH22 HH23
 5K072 AA28 BB02 BB13 CC34 EE03
 GG14